Section 2.1: Proof Techniques

February 2, 2009

Abstract

Sometimes we see patterns in nature and wonder if they hold in general: in such situations we are demonstrating inductive reasoning to propose an **hypothesis**, which may become a **theorem** which we attempt to prove via deductive reasoning. From our work in Chapter 1, we conceive of a theorem as an argument of the form $P \rightarrow Q$, whose validity we seek to demonstrate.

This section outlines a variety of proof techniques, including direct proofs, proofs by contraposition, proofs by contradiction, proofs by exhaustion, and proofs by dumb luck or genius! You have already seen each of these in chapter 1 (with the exception of "dumb luck or genius", perhaps!).

1 Theorems and Informal Proofs

The theorem-forming process is one in which we

- make observations about nature, about a system under study, etc.;
- discover patterns which appear to hold in general;
- state the rule; and then
- attempt to prove it (or disprove it!).

This process is formalized in the following definitions:

- **inductive reasoning** - drawing a conclusion based on experience, which one might state as a conjecture, hypothesis, or theorem.
- **deductive reasoning** - application of a logic system to investigate a proposed conclusion based on hypotheses (hence proving, disproving, or, failing either, holding in limbo the conclusion).
- **counterexample** - an example which violates a proposed rule (or theorem), proving that the rule doesn't work in the particular interpretation.

Before attempting to prove a theorem, we should be convinced of its correctness; if we doubt it, then we should pursue the line of our doubt, and attempt to find a counterexample.

1.1 Exhaustive Proof

- **Example: The Four-color problem**
  - Description (see p. 432).
  - This theorem is partly famous because it provided the first example of a computer-aided proof of a major result. The reason the computer became useful was that the proof came down to testing a rather large number of special cases (proof by exhaustion).

  When there are only a few things (in particular, a finite number) to test, we can use proof by exhaustion.

- **Example: Prolog**, in which we use Horn Clauses, resolution, and a finite number of possibilities (finite database) to decide if a theorem is true.

- **Example: My young friend Sam**

  Kids are wonderful at developing conjectures, and sometimes even applying deductive logic, as illustrated in my friend Sam's Story. Sam made an amazing application of proof by exhaustion.

  Kids will make all sorts of false conjectures (e.g. "All animals living in the ocean are fish," or "all meat-eaters are animals"), and parents, siblings, friends, and teachers all have the priviledge and pleasure of coming up with counterexamples.

1.2 Direct Proof

The most obvious and common technique is the direct proof: you start with your hypotheses $\{P_i\}$, and proceed directly toward your conclusion Q:

$$P_1 \wedge P_2 \wedge \cdots \wedge P_n \rightarrow Q$$

Example: Exercise 12, p. 98 Prove directly that the sum of even integers is even.

$$(\forall x)(\forall y)\left[E(x) \wedge E(y) \rightarrow E(x+y)\right]$$

1. $E(x)$
2. $E(y)$

5. $x + y = 2m + 2n$ — defn of addition
6. $x + y = 2(m+n)$ — distribution

3. $x = 2m$ } def of evenness
4. $y = 2n$

7. $m+n \in \mathbb{Z}$ closure

8. $E(x+y)$ def of evenness

1.3 Contraposition

If $P \to Q$ isn't getting you anywhere, you can use your logic systems to rewrite it as $Q' \to P'$ (the contrapositive). This is called "proof by contraposition".

Example: Practice 4 and 5, p. 94: The statements from chapter

1.1 are:

(a) If the rain continues, then the river will flood.

If the river isn't flooding then the rain stopped.
If the river didn't flood, then the rain didn't continue.

(b) A sufficient condition for $\underbrace{\text{network failure}}_{Q}$ is that $\underbrace{\text{the central switch}}_{P}$ goes down.

If the network doesn't fail, then the central is up.

(c) The avocados are ripe only if they are dark and soft.

(d) A good diet is a necessary condition for a healthy cat.

Example: Exercise 21, p. 99 Prove: If a number x is positive, so is $x+1$.

x+1 not positive → x is not positive

1. $P(x)$
2. $x > 0$
3. $x+1 > 1$
4. $1 > 0$
5. $x+1 > 0$
6. $P(x+1)$

1. $NP(x+1)$
2. $x+1 \le 0$
3. $x \le -1$
4. $-1 \le 0$
5. $x \le 0$
6. $NP(x)$

1.4 Contradiction

Contradiction represents some interesting logic: again, we want to prove $P \to Q$, but rather than proceed directly, we seek to demonstrate that $P \wedge Q' \to 0$: that is, that P and Q' leads to a contradiction. Then we cannot have both P true, and Q false - which would lead to $P \to Q$ false, of course.

$P \to Q$

$P \to (Q \vee 0)$

$P \to (Q' \to 0)$

$P \wedge Q' \to 0$

Example: Exercise 26, p. 99 Prove: If x is an even prime number, then $x = 2$.

x even prime $\wedge$ $x \neq 2 \to 0$

1. x even prime — hyp
2. $x = 2m$ — $m \in \mathbb{Z}$, defn of evenness
3. $x \neq 2$ — hyp
4. $m \neq 1$ (else contradiction: $x = 2$)
5. $m \neq x$ (else $x = 0$, but x prime)
6. $m \mid x$
7. x not prime (divisible by $m \neq 1$ or x) — contradicts x prime
8. 0

QED

Table 1: Summary of useful proof techniques, from Gersting, p. 96.

Proof Technique	Approach to Prove $P \to Q$	Remarks
Exhaustive Proof	Demonstrate $P \to Q$ for all examples/cases.	Examples/cases finite
Direct Proof	Assume P, deduce Q.	Standard approach
Contraposition	Assume Q', deduce P'.	Q' gives more ammo?
Contradiction	Assume $P \wedge Q'$, deduce contradiction.	

1.5 Serendipity

Mathematicians often spend a great deal of time finding the most "elegant" proof of a theorem, or the shortest proof, or the most intuitive proof. We may stumble across a beautiful proof quite by accident ("serendipitously"), and those are perhaps the most pleasant proofs of all. There is a wonderful story associated with Exercise 69, p. 100.

Prove: the sum of the integers from 1 to 100 is 5050.

$1 + 2 + 3 + \ldots 49 + 50 + \ldots + 98 + 99 + 100$

$\underbrace{99 + 98 + 97 + \cdot 51}_{}$

49 pairs that add to 100

$4900 + 50 + 100$

$1 + 2 + 3 + \ldots + 98 + 99 + 100$

$100 + 99 + \ldots \qquad 2 + 1$

$$\frac{100 \cdot 101}{2}$$

$1 + 2 + 3 + \ldots + (n-2) + (n-1) + n$

$n + (n-1) + (n-2) + \ldots + 3 + 2 + 1$

$$\frac{n(n+1)}{2}$$